AF
DW

DE919990082

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Schaeck et al.	Confirmation No.:	1249
Serial No.:	09/731,509	Group Art Unit:	2136
Filed:	12/07/2000	Examiner:	Colin, Carl G.

Title: CONDITIONAL SUPPRESSION OF CARD HOLDER VERIFICATION

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Briefs – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 8, 2006.

Rosalind Q. Spiller

Rosalind Q. Spiller

Date of Signature: May 8, 2006.

05/12/2006 TBESHAH1 00000008 090463 09731509
01 FC:1402 500.00 DA

To: Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPELLANTS' APPEAL BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

This is an appeal under 37 C.F.R. §1.191 and §1.192 from a Final Rejection, mailed on December 6, 2005, of claims 16-47, comprising all the claims finally rejected. A Notice of Appeal was timely filed on March 6, 2006, and received in the U.S. Patent and Trademark Office on March 9, 2006, with an Appeal Brief due May 9, 2006. Therefore, this Brief is being timely

filed. A Transmittal of Appeal Brief is included herewith authorizing the Commissioner to charge the fee for filing this Appeal Brief in the amount of $500 as set forth in 37 C.F.R. §1.17(f).

REAL PARTY IN INTEREST

International Business Machines Corporation, the sole assignee of the inventors' rights in this patent application, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

To the knowledge of Appellants, Appellants' undersigned legal representative, or the assignee, there are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

Claims 1-15 were originally presented in the subject application. Claims 1-15 were cancelled and claims 16-47 added in a Response dated August 4, 2004. Claims 16, 20, 28, 33, 34, 36, 40, 41 and 47 were amended in a Preliminary Amendment filed April 8, 2005, with a Request for Continued Examination. Therefore, claims 16-47 remain in this case, of which all stand rejected as allegedly obvious over Findley, Jr. et al. (U.S. Patent No. 5,979,773) in view of Sloan (U.S. Patent No. 6,179,205).

STATUS OF AMENDMENTS

No amendment was filed subsequent to final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Claim 16 recites a method of controlling card holder verification. The method comprises checking the presence of a trusted association between at least one device and a card usable with the at least one device. See the present application at FIG. 2, elements 210 and 220, and in the text at page 10, line 17 to 25. If the checking indicates the presence of the trusted association, involvement of a holder of the card in performing card holder verification is suppressed. See the present application at FIG. 2, elements 230 and 240, and in the text at page 10, line 25 to page 11, line 6. Otherwise, if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification. See the present application at FIG. 2, elements 250 and 260, and in the text at page 11, lines 7-12.

Claim 19 depends from claim 16, and recites that suppressing card holder involvement comprises performing card holder verification hidden from the holder of the card. As described in the specification at page 10, line 24 to page 11, line 2 (FIG. 2, elements 220 and 230), the Chipcard-ID read from the card is compared to the stored Chipcard-ID's. If the Chipcard-ID is found stored together with a PIN number, the PIN is sent from the terminal to the card. In this way, the user need not enter his or her PIN number.

Claim 20 depends from claim 19, and recites that performing card holder verification hidden from the holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card. As described in the specification at page 10, line 24 to page 11, line 6 (FIG. 2, elements 220, 230 and 240), the Chipcard-ID read from the card is compared to the stored Chipcard-ID's. If the Chipcard-ID is found stored together with a PIN number, the PIN is sent from the terminal to the card. The Chipcard processor then verifies the PIN sent from the terminal. In this way, the PIN is verified without intervention of the user.

Claim 21 depends from claim 16, and recites that suppressing involvement comprises refraining from performing card holder verification. See the present application at page 10, line 24 to page 11, line 6; and FIG. 2.

Claim 22 depends from claim 16, and recites that checking the presence of a trusted association between a device of the at least one device and the card comprises comparing a card identifier stored on the card with one or more card identifiers stored in the device. As described in the specification at page 10, line 24 to page 11, line 2 (FIG. 2, elements 220 and 230), the Chipcard-ID read from the card is compared to the stored Chipcard-ID's. If the Chipcard-ID is found stored together with a PIN number, the PIN is sent from the terminal to the card. In this way, the card ID on the card is compared to that stored in the device.

Claim 25 depends from claim 16, and recites that checking the presence of a trusted association between a device of the at least one device and the card, comprises comparing an

identifier of the device (terminal ID) with one or more device identifiers stored on the card. See FIG. 2, steps 210 and 220, and described in the specification at page 10, line 17 to page 11, line 12.

Claim 28 depends from claim 16 and recites that suppressing involvement comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without requesting information from the holder of the card, and wherein the involving the holder of the card comprises requesting the holder of the card to enter the personal identification number. See steps 230 and 250 of FIG. 2, described in the specification at page 10, line 25 to page 11, line 11.

Claim 32 depends from claim 16 and recites that the checking is between at least one device and a plurality of cards, and that the suppressing is for a plurality of holders. See the specification at page 4, line 23 to page 5, line 4.

Claim 33 recites a method of performing card holder verification. The method comprises checking the presence of a trusted association between at least one device and a card usable with the at least one device. See the present application at FIG. 2, elements 210 and 220, and in the text at page 10, line 17 to 25. The method further comprises performing card holder verification based on the checking: if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card. See the present application at FIG. 2, elements 230 and 240, and in the text at page 10, line 25 to page 11, line 6. However, if the

checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card. See the present application at FIG. 2, elements 250 and 260, and in the text at page 11, lines 7-12.

Claim 34 recites a system of controlling card holder verification. A general description of one example of a system shown in FIG. 1 is given in the specification at page 7, line 19 to page 8, line 16. The system comprises means (processing logic circuit 26, FIG. 1) for checking the presence of a trusted association between at least one device (terminal device 12, FIG. 1) and a card (chipcard 10, FIG. 1) usable with the at least one device; and means (processing logic circuit 26, FIG. 1) for suppressing involvement of a holder of the card in performing card holder verification. If the checking indicates the presence of the trusted association, or for involving the holder of the card in performing card holder verification, if the checking indicates no trusted association. See the summary of claim 16 above for a description of the operation of the system. See the specification also at page 15, line 17 to page 16, line 15 for an example where the processing logic circuit is located on a SIM card of a mobile phone, rather than on the device side.

Claim 40 recites a system of performing card holder verification. A general description of one example of a system shown in FIG. 1 is given in the specification at page 7, line 19 to page 8, line 16. The system comprises at least one processor (processing logic circuit 26, FIG. 1) to perform card holder verification based on whether a trusted association exists between at least one device (terminal device 12, FIG. 1) and a card (chipcard 10, FIG. 1) usable with the at least

one device. If a checking of the trusted association indicates the presence of the trusted association, then a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card. However, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card. See the specification at page 10, line 17 to page 11, line 12.

Claim 41 recites an article of manufacture, comprising at least one computer usable medium having computer readable program code logic to control card holder verification. See the present application at page 17, line 18 to page 18, line 5, describing a computer program product. The computer readable program code logic comprises check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device; and logic to suppress involvement of a holder of the card in performing card holder verification, if the checking indicates the presence of the trusted association, or to involve the holder of the card in performing card holder verification, if the checking indicates no trusted association. See the specification at page 10, line 17 to page 11, line 12.

Claim 47 recites an article of manufacture, comprising at least one computer usable medium having computer readable program code logic to perform card holder verification. See the present application at page 17, line 18 to page 18, line 5, describing a computer program product. The computer readable program code logic comprises check logic to check the presence of a trusted association between at least one device and a card usable with the at least

one device; and perform logic to perform card holder verification based on the checking. If the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card; however, and if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card. See the specification at page 10, line 17 to page 11, line 12.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 16-47 are obvious over Findley, Jr. et al. (U.S. Patent No. 5,979,773) in view of Sloan (U.S. Patent No. 6,179,205).

ARGUMENT

As an initial matter, and explained more fully below, Appellants submit that Sloan teaches away from card holder involvement in verification. As such, Appellants submit Sloan is improperly cited against the claims of the present application. Moreover, given the allegation in the final Office Action that Findley teaches card holder verification, Appellants submit that such opposite teachings would not lead one skilled in the art to combine Sloan with Findley, and that Sloan is improperly combined with Findley.

Claim 16 recites, for example, that "if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification."

In stark contrast, Sloan teaches (emphasis added) at column 2, lines 33-51:

> Some smart card companies, such as Mondex International, currently utilize a wallet which can lock and unlock a smart card. The locking and unlocking mechanism utilizes a personal identification number (PIN) to ensure authenticity of the lock or unlock request. However, **many people prefer not to use PINs**. It is a **nuisance** to have to memorize a PIN, particularly if the person already has several PINs memorized. Additionally, a particular **PIN can be forgotten or confused** with another PIN. Further, the need for a PIN requires that the "electronic wallet" device has at least a numeric key pad to enter the PIN. This is **undesirable** for some users who do not want to carry a relatively bulky wallet with them.
>
> What is needed is a system and method for automatically ensuring authenticity for locking and unlocking an application in a smart card which does not require the user to memorize a PIN. Preferably, the system and method may be implemented using a device which does not require the use of a bulky and expensive keypad.

Thus, Appellants submit that Sloan teaches away from card holder involvement in the verification process, and thus, teaches away from the presently claimed invention. Moreover, given the Office Action allegation that Findley teaches card holder involvement, Appellants submit these opposing teachings have two consequences. First, one skilled in the art would not be motivated to combine Sloan with Findley, and second, the combination of Sloan with Findley is improper.

Claim 16

Findley teaches a dual card system where an access card is necessary to access data on an identity/user card. See, e.g., Findley at column 3, lines 42-51. Each card is given to different

people, the access card being given to a system operator and the identity/user card being given to a user. Findley teaches at column 4 that access cards can be made to expire and/or use a PIN/password.

Appellants submit Findley fails to teach or suggest conditional card holder verification as claimed. The disclosure in column 4 of Findley regarding access cards using a PIN/password is not conditioned on anything, let alone the claimed trusted association between the device and the card. A PIN/password is either implemented as part of the Findley system, or it is not. There is nothing conditional about it. With regard to access card expiration, Findley simply generally teaches that reactivation following system sponsor/operator procedures is necessary. There is no disclosure, teaching or suggestion as to what the reactivation procedure would be.

Moreover, Appellants submit that one of ordinary skill would not view a date for expiration as being a trusted association. Examples of a trusted association given in the application (and claimed—see, e.g., claim 25) include checking a device ID against that stored on the card, and checking a card ID against that stored on the device. A mere expiration date has no trust aspect in the sense of one entity knowing or recognizing another. However, even if an expiration date were somehow held to read on a trusted association, Appellants submit access card holder verification is not taught, only reactivation according to an undescribed procedure with nothing more.

Even ignoring the above remarks regarding Sloan teaching away from user involvement, Appellants submit Sloan does not overcome the deficiencies of Findley. Similar to Findley,

Sloan fails to disclose, teach or suggest a conditional card holder verification procedure in which intervention is suppressed, if there is a presence of a trusted association, but intervention is used, if such a trusted association does not exist. That is, there is no disclosure, teaching or suggestion in Sloan of suppressing involvement of a card holder in performing card holder verification in the event there is a trusted association, and if there is no trusted association, going forward with card holder verification, but requiring card holder intervention.

In Sloan, the smart card device either issues an unlock command, if it has cached a password for the card identifier, or indicates that it is unable to unlock the application on the smart card if it has no entry for the card. It does not involve the holder of the card in card holder verification if there is no trusted association, as claimed by Appellants. Thus, Appellants respectfully submit that Sloan does not disclose, teach or suggest one or more aspects of Appellants' claimed invention.

Since both Findley and Sloan fail to describe, teach or suggest the conditional aspect of Appellants' claimed invention in which involvement of the card holder in performing card holder verification is suppressed, if a trusted association is present, and card holder intervention is used in the card holder verification, if there is no trusted association, Appellants respectfully submit that the combination of Findley and Sloan fails to teach or suggest one or more aspects of the present invention.

The final Office Action also maintains generally that it is well known in the art that when checking indicates no trusted association, involving the card holder to perform verification. In

support, the final Office Action cited to Creekmore (U.S. Patent No. 4,187,498) at column 6, lines 39-67, and generally to Beuk et al. (U.S. Patent No. 5,446,266). Appellants respectfully disagree for the reasons detailed below.

Creekmore discloses a check verification system that includes an ID card. However, the checking that is being done in Creekmore is not checking for a trusted association between a device and a card usable with the device. Instead, Creekmore checks for card usability, i.e., checks to see if the card is a check cashing card. No trusted association as claimed is checked. Moreover, Creekmore teaches that an ID number is always requested for check cashing cards.

Similar to Findley, Beuk et al. discloses a dual card system, one having a system code and the other a security code. Any card with the correct security code can operate the apparatus, and the card with the system code can change the security code on the security card. If the security code is not correct, the apparatus cannot be used. The final Office Action cites to no specific section of Beuk et al., however, the Advisory Action of February 17, 2006 cites to FIG. 2 of Beuk et al. However, FIG. 2 and the description thereof merely teaches checking for the correct code on a card. If the correct code is found, the user is given an opportunity to reset the code. Appellants submit this is not conditional card holder involvement in card holder verification.

Therefore, Appellants submit that claim 16 cannot be rendered obvious over Findley in view of Sloan.

Each of independent claims 33, 34, 40, 41 and 47 contains, in some form, limitations similar to that argued above with respect to claim 16. Thus, the remarks made above with respect to claim 16 are equally applicable thereto. Therefore, each of claims 33, 34, 40, 41 and 47 also cannot be made obvious over Findley in view of Sloan.

Claim 19

The final Office Action does not specifically address claim 19. However, Appellants could find no disclosure, teaching or suggestion of card holder verification hidden from the card holder. As remarked above, Findley mentions PIN/password protection and card expiration, but provides no details. Of course, user entry of a PIN or password is not hidden from the card holder, and for card expiration, Findley is simply silent on what the reactivation procedure is, or who would be doing it. Sloan does not remedy the shortcomings of Findley in this regard.

Therefore, Appellants submit that claim 19 cannot be rendered obvious over Findley in view of Sloan.

Claims 35, 42 contain a limitation similar to that argued above with respect to claim 19. Thus, the remarks above apply equally thereto, and claims 35 and 42 also cannot be obviated over Findley in view of Sloan.

Claim 20

Against claim 20, the final Office Action cites to Findley at column 7, lines 14-67. However, that section teaches that identity information is read and displayed from an identity

card if the access and identity cards are compatible as to accessible fields of data. There is no PIN involved, and, in any case, the claimed association is between the device and the card, not two cards. Against claim 20, the final Office Action next cites to Findley at column 2, lines 1-30. However, that section teaches comparing secured area access data on the two cards to determine if the identity card has access to a given area. Again, no teaching regarding a PIN or card *holder* verification, much less verifying a PIN hidden from and without intervention of the user. Next, the final Office Action cites to Findley at column 2, lines 35-58. However, that section teaches that the access card can add/modify digital identity data regarding the user. Again, nothing regarding a PIN, card holder verification, or obtaining/verifying PIN hidden from and without intervention of the user. Finally, the final Office Action cites to Findley at column 7, lines 10-20. However, that section merely teaches that identity cards contain digital identity data regarding the user.

Therefore, Appellants submit that claim 20 cannot be rendered obvious over Findley in view of Sloan.

Claims 28, 33, 36, 40, 43 and 47 contain a limitation similar to that argued above with respect to claim 20. Thus, the remarks above apply equally thereto, and claims 28, 33, 36, 40, 43 and 47 also cannot be obviated over Findley in view of Sloan.

Claim 21

Against claim 21, the final Office Action first cites to Findley at column 7, lines 14-67. However, that section teaches that identity information is read and displayed from an identity

card if the access and identity cards are compatible as to accessible fields of data. The final Office Action next cites to Findley at column 2, lines 1-30. However, that section teaches comparing secured area access data on the two cards to determine if the identity card has access to a given area. Next, the final Office Action cites to Findley at column 2, lines 35-58. However, that section teaches that the access card can add/modify digital identity data regarding the user. Finally, the final Office Action cites to Findley at column 7, lines 10-20. However, that section merely teaches that identity cards contain digital identity data regarding the user. Appellants submit that none of the cited sections teaches or suggests refraining from performing card holder verification, as claimed in claim 21.

Therefore, Appellants submit that claim 21 cannot be rendered obvious over Findley in view of Sloan.

Claims 37 and 44 contain limitations similar to that argued above with respect to claim 21. Thus, the remarks above apply equally thereto, and claims 37 and 44 also cannot be obviated over Findley in view of Sloan.

Claim 22

Against claim 22, the final Office Action first cites to Findley at column 7, lines 14-67. However, that section teaches that identity information is read and displayed from an identity card if the access and identity cards are compatible as to accessible fields of data. The final Office Action next cites to Findley at column 2, lines 1-30. However, that section teaches comparing secured area access data on the two cards to determine if the identity card has access

to a given area. Next, the final Office Action cites to Findley at column 2, lines 35-58. However, that section teaches that the access card can add/modify digital identity data regarding the user. Finally, the final Office Action cites to Findley at column 7, lines 10-20. However, that section merely teaches that identity cards contain digital identity data regarding the user. Appellants submit that none of the cited sections teaches or suggests comparing a card identifier on the card with one or more stored in the device. At most, Findley compares access information stored on two cards, not a card and a machine, and not a card identifier.

Therefore, Appellants submit that claim 22 cannot be rendered obvious over Findley in view of Sloan.

Claims 38 and 45 contain limitations similar to that argued above with respect to claim 22. Thus, the remarks above apply equally thereto, and claims 38 and 45 also cannot be obviated over Findley in view of Sloan.

Claim 25

Against claim 25, the final Office Action cites to the rejections of claims 22, 23 and 26. However, of those, only the rejection of claim 22 seems even remotely relevant. The teaching of each section of Findley cited against claim 22 is discussed above. However, Appellants submit that none of the sections teaches or suggests comparing an identifier of the device with one or more device identifiers stored on the card. At most, Findley compares access information stored on two cards, not a machine and a card, and not a device identifier.

Therefore, Appellants submit that claim 25 cannot be rendered obvious over Findley in view of Sloan.

Claims 39 and 46 contains a limitation similar to that argued above with respect to claim 25. Thus, the remarks above apply equally thereto, and claim 39 and 46 also cannot be obviated over Findley in view of Sloan.

Claim 28

As best Appellants can tell, since many claims were not individually addressed, the final Office Action cites to Findley at column 7, lines 14-67 and column 8, lines 50-67, against claim 28. However, the first section teaches that identity information is read and displayed from an identity card if the access and identity cards are compatible as to accessible fields of data. There is no PIN involved. In addition, the second cited section teaches that an access card can have different levels of security, allowing the holder to view different information on another holder's identity card. Again, there is no PIN involved. Appellants also submit that Sloan fails to remedy the noted shortcomings of Findley, since Sloan only addresses locking and unlocking applications.

Therefore, Appellants submit that claim 28 cannot be rendered obvious over Findley in view of Sloan.

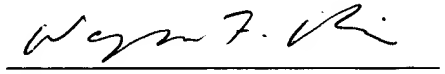
Claim 32

Against claim 32, the final Office Action cites to Findley at FIG. 11. A review of the detailed description of Findley reveals no mention of FIG. 11. Appellants submit that what is shown in FIG. 11 is one card accessing other cards over a network, and not the claimed checking for a trusted association between at least one device and a plurality of cards or suppressing involvement of a plurality of card holders in card holder verification.

Therefore, Appellants submit that claim 28 cannot be rendered obvious over Findley in view of Sloan.

Appellants submit that the dependent claims not specifically addressed herein are allowable for the same reasons as the independent claims from which they directly or ultimately depend.

In conclusion, Appellants submit that none of claims 16-47 is obvious over Findley in view of Sloan. Therefore, Appellants submit that the final Office Action should be reversed in all respects.



Wayne F. Reinke
Attorney for Appellants
Registration No.: 36,650

Dated: May 8, 2006.

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203-5160
Telephone: (518) 452-5600
Facsimile: (518) 452-5579

CLAIMS APPENDIX

1-15. (Canceled).

16. (Previously Presented) A method of controlling card holder verification, said method comprising:

checking the presence of a trusted association between at least one device and a card usable with the at least one device; and

if the checking indicates the presence of the trusted association, then suppressing involvement of a holder of the card in performing card holder verification, otherwise, if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification.

17. (Previously Presented) The method of claim 16, wherein the at least one device is located in a trusted environment.

18. (Previously Presented) The method of claim 16, wherein the card comprises a chipcard.

19. (Previously Presented) The method of claim 16, wherein the suppressing involvement comprises performing card holder verification hidden from the holder of the card.

20. (Previously Presented) The method of claim 19, wherein the performing card holder verification hidden from the holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card.

21. (Previously Presented) The method of claim 16, wherein the suppressing involvement comprises refraining from performing card holder verification.

22. (Previously Presented) The method of claim 16, wherein the checking the presence of a trusted association between a device of the at least one device and the card comprises comparing a card identifier stored on the card with one or more card identifiers stored in the device.

23. (Previously Presented) The method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprises replacing the personal identification number with another personal identification number.

24. (Previously Presented) The method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprises erasing the association between the card identifier and the personal identification number.

25. (Previously Presented) The method of claim 16, wherein the checking the presence of a trusted association between a device of the at least one device and the card comprises comparing an identifier of the device with one or more device identifiers stored on the card.

26. (Previously Presented) The method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, and said method further comprises replacing the personal identification number with another personal identification number.

27. (Previously Presented) The method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, and said method further comprises erasing the association between the device identifier and the personal identification number.

28. (Previously Presented) The method of claim 16, wherein the suppressing involvement comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without requesting information from the holder of the card, and wherein the involving the holder of the card comprises requesting the holder of the card to enter the personal identification number.

29. (Previously Presented) The method of claim 16, further comprising associating the at least one device and the card.

30. (Previously Presented) The method of claim 29, further comprising controlling the association between a device of the at least one device and the card.

31. (Previously Presented) The method of claim 30, wherein the controlling comprises using a network connectable to the device.

32. (Previously Presented) The method of claim 16, wherein the checking is between at least one device and a plurality of cards, and wherein the suppressing is for a plurality of holders.

33. (Previously Presented) A method of performing card holder verification, said method comprising:

checking the presence of a trusted association between at least one device and a card usable with the at least one device; and

performing card holder verification based on the checking, wherein:

if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card;

however, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card.

34. (Previously Presented) A system of controlling card holder verification, said system comprising:

means for checking the presence of a trusted association between at least one device and a card usable with the at least one device; and

means for suppressing involvement of a holder of the card in performing card holder verification, if the checking indicates the presence of the trusted association, or for involving the holder of the card in performing card holder verification, if the checking indicates no trusted association.

35. (Previously Presented) The system of claim 34, wherein the means for suppressing involvement comprises means for performing card holder verification hidden from the holder of the card.

36. (Previously Presented) The system of claim 35, wherein the means for performing card holder verification hidden from the holder of the card comprises means for automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card.

37. (Previously Presented) The system of claim 34, wherein the means for suppressing involvement comprises refraining from performing card holder verification.

38. (Previously Presented) The system of claim 34, wherein the means for checking the presence of a trusted association between a device of the at least one device and the card comprises means for comparing a card identifier stored on the card with one or more card identifiers stored in the device.

39. (Previously Presented) The system of claim 34, wherein the means for checking the presence of a trusted association between a device of the at least one device and the card comprises means for comparing an identifier of the device with one or more device identifiers stored on the card.

40. (Previously Presented) A system of performing card holder verification, said system comprising:

at least one processor to perform card holder verification based on whether a trusted association exists between at least one device and a card usable with the at least one device, wherein:

if a checking of the trusted association indicates the presence of the trusted association, then a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card;

however, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card.

41. (Previously Presented) An article of manufacture comprising:

at least one computer usable medium having computer readable program code logic to control card holder verification, the computer readable program code logic comprising:

check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device; and

logic to suppress involvement of a holder of the card in performing card holder verification, if the checking indicates the presence of the trusted association, or to involve the holder of the card in performing card holder verification, if the checking indicates no trusted association.

42. (Previously Presented) The article of manufacture of claim 41, wherein the suppress logic to suppress involvement comprises perform logic to perform card holder verification hidden from the holder of the card.

43. (Previously Presented) The article of manufacture of claim 42, wherein the perform logic comprises obtain logic to automatically obtain a personal identification number of the holder of the card and verify logic to verify the personal identification number without intervention of the holder of the card.

44. (Previously Presented) The article of manufacture of claim 41, wherein the suppress logic to suppress involvement comprises refrain logic to refrain from performing card holder verification.

45. (Previously Presented) The article of manufacture of claim 41, wherein the check logic to check the presence of a trusted association between a device of the at least one device and the card comprises compare logic to compare a card identifier stored on the card with one or more card identifiers stored in the device.

46. (Previously Presented) The article of manufacture of claim 41, wherein the check logic to check the presence of a trusted association between a device of the at least one device and the card comprises compare logic to compare an identifier of the device with one or more device identifiers stored on the card.

47. (Previously Presented) An article of manufacture comprising:

at least one computer usable medium having computer readable program code logic to perform card holder verification, the computer readable program code logic comprising:

check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device; and

perform logic to perform card holder verification based on the checking, wherein:

if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card;

however, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No.
DE919990082

In Re Application Of: **Schaeck et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/731,509	12/07/2000	Colin, Carl G.	46369	2136	1249

Invention: **CONDITIONAL SUPPRESSION OF CARD HOLDER VERIFICATION**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:

The fee for filing this Appeal Brief is: **$500.00**

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 09-0463 (IBM) . I have enclosed a duplicate copy of this sheet.

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Wayne F. Reinke

Signature

Dated: **May 8, 2006**

Wayne F. Reinke, Esq.
Registration No. 36,650

Heslin Rothenberg Farley & Mesiti P.C.
5 Columbia Circle
Albany, NY 12203
Telephone: 518-452-5600
Facsimile: 518-452-5579

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

May 8, 2006
(Date)

Rosalind Q. Spiller

Signature of Person Mailing Correspondence

Rosalind Q. Spiller

Typed or Printed Name of Person Mailing Correspondence

cc: